CCNP®: Cisco Internetwork Troubleshooting Study Guide

Arthur Pfund
Todd Lammle

SYBEX®

CCNP:
Cisco Internetwork Troubleshooting
Study Guide

CCNP®:
Cisco Internetwork Troubleshooting
Study Guide

Arthur Pfund

Todd Lammle

San Francisco • London

SYBEX

SYBEX and the SYBEX logo are either registered trademarks or trademarks of SYBEX Inc. in the United States and/or other countries.

Screen reproductions produced with FullShot 99. FullShot 99 © 1991-1999 Inbit Incorporated. All rights reserved. FullShot is a trademark of Inbit Incorporated.

The CD interface was created using Macromedia Director, COPYRIGHT 1994, 1997-1999 Macromedia Inc. For more information on Macromedia and Macromedia Director, visit http://www.macromedia.com.

This study guide and/or material is not sponsored by, endorsed by or affiliated with Cisco Systems, Inc. Cisco ®, Cisco Systems ®, CCDA , CCNA , CCDP , CCSP, CCIP, BSCI, CCNP , CCIE , CCSI , the Cisco Systems logo and the CCIE logo are trademarks or registered trademarks of Cisco Systems, Inc. in the United States and certain other countries. All other trademarks are trademarks of their respective owners.

TRADEMARKS: SYBEX has attempted throughout this book to distinguish proprietary trademarks from descriptive terms by following the capitalization style used by the manufacturer.

The author and publisher have made their best efforts to prepare this book, and the content is based upon final release software whenever possible. Portions of the manuscript may be based upon pre-release versions supplied by software manufacturer(s). The author and the publisher make no representation or warranties of any kind with regard to the completeness or accuracy of the contents herein and accept no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages of any kind caused or alleged to be caused directly or indirectly from this book.

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

SYBEX

To Our Valued Readers:

Thank you for looking to Sybex for your CCNP certification exam prep needs. We at Sybex are proud of the reputation we've established for providing certification candidates with the practical knowledge and skills needed to succeed in the highly competitive IT marketplace. Sybex is proud to have helped thousands of Cisco certification candidates prepare for their exams over the years, and we are excited about the opportunity to continue to provide computer and networking professionals with the skills they'll need to succeed in the highly competitive IT industry.

We at Sybex are proud of the reputation we've established for providing certification candidates with the practical knowledge and skills needed to succeed in the highly competitive IT marketplace. It has always been Sybex's mission to teach individuals how to utilize technologies in the real world, not to simply feed them answers to test questions. Just as Cisco is committed to establishing measurable standards for certifying those professionals who work in the cutting-edge field of internetworking, Sybex is committed to providing those professionals with the means of acquiring the skills and knowledge they need to meet those standards.

The author and editors have worked hard to ensure that the Study Guide you hold in your hand is comprehensive, in-depth, and pedagogically sound. We're confident that this book will exceed the demanding standards of the certification marketplace and help you, the Cisco certification candidate, succeed in your endeavors.

As always, your feedback is important to us. Please send comments, questions, or suggestions to support@sybex.com. At Sybex we're continually striving to meet the needs of individuals preparing for IT certification exams.

Good luck in pursuit of your CCNP certification!

Neil Edde
Associate Publisher—Certification
Sybex, Inc.

To my parents for helping me become the person I am today.

Acknowledgments

Contents at a Glance

Table of Contents

Introduction

This book is intended to help you continue on your exciting new path toward obtaining your CCNP certification. Before reading this book, it is important to have at least read the Sybex *CCNA: Cisco Certified Network Associate Study Guide*, Fourth Edition. You can take the CCNP tests in any order, but you should have passed the CCNA exam before pursuing your CCNP. Many questions in the Cisco Internet Troubleshooting Support (CIT) exam are built on the CCNA material. However, we have done everything possible to make sure that you can pass the CIT exam by reading this book and practicing with Cisco routers.

Cisco Systems's Place in Networking

Cisco Systems has become an unrivaled worldwide leader in networking for the Internet. Its networking solutions can easily connect users who work from diverse devices on disparate networks. Cisco products make it simple for people to access and transfer information without regard to differences in time, place, or platform.

Cisco Systems's big picture is that it provides end-to-end networking solutions that customers can use to build an efficient, unified information infrastructure of their own or to connect to someone else's. This is an important piece in the Internet/networking-industry puzzle, because a common architecture that delivers consistent network services to all users is now a functional imperative. Because Cisco Systems offers such a broad range of networking and Internet services and capabilities, users needing regular access to their local network or the Internet can do so unhindered, making Cisco's wares indispensable.

Cisco answers this need with a wide range of hardware products that are used to form information networks using the Cisco Internetworking Operating System (IOS) software. This software provides network services, paving the way for networked technical support and professional services to maintain and optimize all network operations.

Along with the Cisco IOS, one of the services Cisco created to help support the vast amount of hardware it has engineered is the Cisco Certified Internetworking Expert (CCIE) program, which was designed specifically to equip people to effectively manage the vast quantity of installed Cisco networks. The business plan is simple: If you want to sell more Cisco equipment and have more Cisco networks installed, ensure that the networks you installed run properly.

However, having an extraordinary product line isn't all it takes to guarantee the huge success that Cisco enjoys—lots of companies with great products are now defunct. If you have complicated products designed to solve complicated problems, you need knowledgeable people who are fully capable of installing, managing, and troubleshooting those products. That part isn't easy, so Cisco began the CCIE program to equip people to support these complicated networks. This program, known colloquially as the Doctorate of Networking, has also been very successful, primarily due to its extreme difficulty. Cisco continually monitors the program, making the changes needed to make sure that the program remains pertinent and accurately reflects the demands of today's internetworking business environments.

Building on the highly successful CCIE program, Cisco Career Certifications permit you to become certified at various levels of technical proficiency, spanning the disciplines of network design and support. So, whether you're beginning a career, changing careers, securing your present position, or seeking to refine and promote your position, this is the book for you!

Cisco's Certifications

Cisco has created several certification tracks that will help you become a CCIE, as well as aid prospective employers in measuring skill levels. Before these new certifications existed, you took only one test and were then faced with the lab, which made it difficult to succeed. With the new certifications that add a better approach to preparing for that almighty lab, Cisco has opened doors that few were allowed through before. So, what are these new certifications, and how do they help you get your CCIE?

Cisco Certified Network Associate (CCNA)

The CCNA certification is the first certification in the new line of Cisco certifications and is a precursor to all current Cisco certifications. With the new certification programs, Cisco has created a type of stepping-stone approach to CCIE certification. Now, you can become a Cisco Certified Network Associate for the meager cost of the Sybex *CCNA: Cisco Certified Network Associate Study Guide*, Fourth Edition, plus $125 for the test.

And you don't have to stop there—you can choose to continue with your studies and select a specific track to follow. The Installation and Support track will help you prepare for the CCIE Routing and Switching certification; the Communications and Services track will help you prepare for the CCIE Communication and Services certification. It is important to note that you do not have to attempt any of these tracks to reach the CCIE, but choosing a track is recommended for the best success.

Cisco Certified Network Professional (CCNP)

The Cisco Certified Network Professional (CCNP) certification has opened many opportunities for the individual wishing to become Cisco-certified but who is lacking the training, the expertise, or the bucks to pass the notorious and often-failed two-day Cisco torture lab. The new Cisco certifications will truly provide exciting new opportunities for the CNE and MCSE who don't see an obvious way to advance.

So, you're thinking, "Great, what do I do after I pass the CCNA exam?" Well, if you want to become a CCIE in Routing and Switching (the most popular certification), understand that there's more than one path to the CCIE certification. One way is to continue studying and become a Cisco Certified Network Professional (CCNP). That means taking four more tests in addition to obtaining the CCNA certification.

> **NOTE** We'll discuss requirements for the CCIE exams later on in this introduction.

> **TIP** Remember that you don't need to be a CCNP or even a CCNA to take the CCIE lab, but to accomplish that, it's extremely helpful if you already have these certifications.

The CCNP program will prepare you to understand and comprehensively tackle the internetworking issues of today and beyond—not limited to the Cisco world. You will undergo metamorphosis, vastly increasing your knowledge and skills through the process of obtaining these certifications.

What Are the CCNP Certification Skills?

Cisco demands a certain level of proficiency for its CCNP certification. In addition to what's required for the CCNA, you'll need to have the following skills:

- Installing, configuring, operating, and troubleshooting complex routed LAN, routed WAN, and switched LAN networks, and Dial Access Services.

- Understanding complex networking concepts, such as IP, IGRP, Async Routing, extended access lists, IP RIP, route redistribution, route summarization, OSPF, VLSM, BGP, Serial, IGRP, Frame Relay, ISDN, ISL, X.25, DDR, PSTN, PPP, VLANs, Ethernet, ATM LAN emulation, access lists, 802.10, FDDI, and transparent and translational bridging.

To meet the Cisco Certified Network Professional requirements, you must be able to perform the following:

- Install and/or configure a network to increase bandwidth, quicken network response times, and improve reliability and quality of service.

- Maximize performance through campus LANs, routed WANs, and remote access.

- Improve network security.

- Create a global intranet.

- Provide access security to campus switches and routers.

- Provide increased switching and routing bandwidth—end-to-end resiliency services.

- Provide custom queuing and routed priority services.

How Do You Become a CCNP?

After becoming a CCNA, the four exams you must take to get your CCNP are as follows:

Exam 642-801: Building Scalable Cisco Internetworks (BSCI)   A while back, Cisco retired the Routing (640-603) exam and now uses this exam, 642-801, to build on the fundamentals of the CCNA exam. BSCI focuses on large multiprotocol internetworks and how to manage them. The BSCI exam is also a required exam for the CCIP and CCDP certifications, which will be discussed later in this introduction.

Exam 642-811: Building Cisco Multilayer Switched Networks (BCMSN)   The Building Cisco Multilayer Switched Networks exam tests your knowledge of the 1900 and 5000 series of Catalyst switches. You'll also be challenged on your knowledge of switching technology, implementation and operation, planning and design.

Exam 642-821: Building Cisco Remote Access Networks (BCRAN)   The Building Cisco Remote Access Networks (BCRAN) exam tests your knowledge of installing, configuring, monitoring, and troubleshooting Cisco ISDN and dial-up access products. You must understand PPP, ISDN, Frame Relay, and authentication.

Exam 642-831: Cisco Internetwork Troubleshooting Support (CIT)   The Cisco Internetwork Troubleshooting Support (CIT) exam tests you on troubleshooting information. You must be able to document a network; troubleshoot Ethernet LANS and IP networks, as well as ISDN, PPP, and Frame Relay networks. This book covers all the topics you'll need to pass the CIT exam.

An Alternate Plan

If you hate tests, you can take fewer of them by signing up for the CCNA exam and the CIT exam, and then take just one more long exam called the Foundation R/S exam (640-841). Doing this also gives you your CCNP—but beware, it's a really long test that fuses all the material listed previously in this introduction into one exam. Good luck! That said, by taking this exam you get three tests for the price of two, which saves you $125 (if you pass). Some people think it's easier to take the Foundation R/S exam because you can leverage your higher-scoring areas against the areas in which you don't do as well. There is also an option to obtain your CCNP. This is to do three tests: the Composite Exam (642-891), which fuses the BSCI and BCMSN exams, plus the BCRAN and CIT exams.

> Remember that test objectives and tests can change at any time without notice. Always check the Cisco website for the most up-to-date information (www.cisco.com).

Sybex has a solution for each one of the CCNP exams. Each study guide listed in the following table covers all the exam objectives for their respective exams.

Exam Name	Exam #	Sybex Products
Building Scalable Cisco Internetworks	642-801	CCNP: *Building Scalable Cisco Internetworks Study Guide* (ISBN 0-7821-4293-1)
Switching	642-811	CCNP: *Building Cisco Multilayer Switched Networks Study Guide* (0-7821-4294-X)
Remote Access	642-821	CCNP: *Building Cisco Remote Access Networks Study Guide* (0-7821-4296-6)
Support	642-831	CCNP: *Cisco Internetwork Troubleshooting Study Guide*. (0-7821-4295-8)

Also available: *CCNP Study Guide Kit, 3rd Ed.* (0-7821-4297-4); covers all four exams.

Cisco Certified Internetwork Professional (CCIP)

After passing the CCNA, the next step in the Communications and Services track is the CCIP. The CCIP is a professional-level certification.

The CCIP certification gives you the skills necessary to understand and tackle the complex internetworking world of the service provider. You will acquire the knowledge necessary to prepare you for moving forward toward the coveted CCIE Communications and Services certification.

What Are the CCIP Certification Skills?

Cisco demands a certain level of proficiency for its CCIP certification. In addition to what's required for the CCNA, you will need to have the following skills:

▪ Performing complex planning, operations, installations, implementations, and trouble-shooting of internetworks.

▪ Understanding and managing complex communications networks—last mile, edge, or core.

How Do You Become a CCIP?

After becoming a CCNA, you must take two core exams and an elective. The core exams are:

Exam 642-801: Building Scalable Cisco Internetworks (BSCI) A while back, Cisco retired the Routing (640-603) exam and now uses this exam, 642-801, to build on the fundamentals of the CCNA exam. BSCI focuses on large multiprotocol internetworks and how to manage them.

Exam 642-641: Quality of Services (QoS) This exam tests your knowledge of Quality of Service for internetworks.

Exam 640-910: Implementing Cisco MPLS (MPLS) This exam tests your knowledge of multiprotocol label switching and its implementation. The Sybex *CCIP: MPLS Study Guide* (ISBN 0-7821-4096-3) covers all the exam objectives.

Exam 642-661: Border Gateway Protocol (BGP) This exam tests your knowledge of Border Gateway Protocol (BGP). When you complete this exam you should be able to manage a large BGP network.

Cisco's Network Design and Installation Certifications

In addition to the Network Installation and Support track and the Communications and Services track, Cisco has created another certification track for network designers. The two certifications within this track are the Cisco Certified Design Associate (CCDA) and Cisco Certified Design Professional (CCDP). If you're reaching for the CCIE stars, we highly recommend the CCNP and CCDP certifications before attempting the CCIE R/S Qualification exam.

These two certifications will give you the knowledge to design routed LAN, routed WAN, and switched LAN.

Cisco Certified Design Associate (CCDA)

To become a CCDA, you must pass the DESGN (Designing for Cisco Internetwork Solutions) test (640-861). To pass this test, you must understand how to do the following:

▪ Design simple routed LAN, routed WAN, and switched LAN and ATM LANE networks.

▪ Use network-layer addressing.

▪ Filter with access lists.

▪ Use and propagate VLAN.

▪ Size networks.

Cisco Certified Design Professional (CCDP)

If you're already a CCNP and want to get your CCDP, you can simply take the ARCH 642-871 test. If you're not yet a CCNP, however, you must take the CCDA, CCNA, BSCI, Switching, Remote Access, and CID exams.

CCDP certification skills include:

- Designing complex routed LAN, routed WAN, and switched LAN and ATM LANE networks.
- Technical knowledge beyond the base level of CCDA.

CCDPs must also demonstrate proficiency in the following:

- Network-layer addressing in a hierarchical environment.
- Traffic management with access lists.
- Hierarchical network design.
- VLAN use and propagation.
- Performance considerations: required hardware and software; switching engines; memory, cost, and minimization.

Cisco's Security Certifications

Quite a few Cisco security certifications are available. All of the Cisco security certifications also require a valid CCNA.

Cisco Certified Security Professional (CCSP)

You have to pass five exams to get your CCSP. The pivotal exam is the SECUR. Here are the exams you must pass to call the CCSP yours:

Exam 642-501: Securing Cisco IOS Networks (SECUR)   This exam tests your understanding of such concepts as basic router security, AAA security for Cisco routers and networks, Cisco IOS Firewall configuration and authentication, building basic and advanced IPSec VPNs, and managing Cisco enterprise VPN routers. Sybex can help you pass the SECUR exam with the *CCSP: Securing Cisco IOS Networks Study Guide* (ISBN 0-7821-4231-1).

Exam 642-521: Cisco Secure PIX Firewall Advanced (CSPFA)   This exam challenges your knowledge of the fundamentals of Cisco PIX Firewalls, as well as translations and connections, object grouping, advanced protocol handling and authentication, authorization, and accounting, among other topics. You can tackle the CSPFA exam with the help of Sybex's *CCSP: Secure PIX and Secure VPN Study Guide* (ISBN 0-7821-4287-7).

Exam 642-511: Cisco Secure Virtual Private Networks (CSVPN)   The CSVPN exam covers the basics of Cisco VPNs; configuring various Cisco VPNs for remote access, hardware client, backup server, and load balancing; plus IPSec over UDP and IPSec over TCP. Again, using the Sybex *CCSP: Secure PIX and Secure VPN Study Guide* (ISBN 0-7821-4287-7), you'll approach the CSVPN exam with confidence.

Exam 642-531: Cisco Secure Intrusion Detection System (CSIDS)   The CSIDS exam will challenge your knowledge of intrusion detection technologies and solutions, and test your abilities to install and configure ISD components. You'll also be tested on managing large-scale

deployments of Cisco IDS sensors using Cisco IDS management software. Prepare for the CSIDS exam using Sybex's *CCSP: Secure Intrusion Detection and SAFE Implementation Study Guide* (ISBN 0-7821-4288-5).

Exam 9E0-131: Cisco SAFE Implementation (CSI)   This exam tests such topics as security and architecture fundamentals, SAFE Network design for small and medium corporate and campus situations, and SAFE remote-user network implementation. You can take advantage of Sybex's *CCSP: Secure PIX and Secure VPN Study Guide* (ISBN 0-7821-4287-7) for help with this exam.

Cisco Firewall Specialist

Cisco Security certifications focus on the growing need for knowledgeable network professionals who can implement complete security solutions. Cisco Firewall Specialists focus on securing network access using Cisco IOS Software and Cisco PIX Firewall technologies.

The two exams you must pass to achieve the Cisco Firewall Specialist certification are Securing Cisco IOS Networks (SECUR) and Cisco Secure PIX Firewall Advanced (CSPFA).

Cisco IDS Specialist

Cisco IDS Specialists can both operate and monitor Cisco IOS Software and IDS technologies to detect and respond to intrusion activities.

The two exams you must pass to achieve the Cisco IDS Specialist certification are Securing Cisco IOS Networks (SECUR) and Cisco Secure Intrusion Detection System (CSIDS).

Cisco VPN Specialist

Cisco VPN Specialists can configure VPNs across shared public networks using Cisco IOS Software and Cisco VPN 3000 Series Concentrator technologies.

The exams you must pass to achieve the Cisco VPN Specialist certification are Securing Cisco IOS Networks (SECUR) and Cisco Secure Virtual Networks (CSVPN).

Cisco Certified Internetwork Expert (CCIE)

Cool! You've become a CCNP, and now your sights are fixed on getting your Cisco Certified Internetwork Expert (CCIE) certification. What do you do next? Cisco recommends a *minimum* of two years on-the-job experience before taking the CCIE lab. After jumping those hurdles, you then have to pass the written CCIE Exam Qualifications before taking the actual lab.

There are four CCIE certifications, and you must pass a written section and a lob portion for each certification. As can be seen from below, most of the CCIE certifications require only a single test, but one requires multiple:

CCIE Communications and Services (Exams 350-020, 350-021, 350-022, 350-023)   The four CCIE Communications and Services written exams cover IP and IP routing, optical, DSL, dial, cable, wireless, WAN switching, content networking, and voice.

CCIE Routing and Switching (Exam 350-001)   The CCIE Routing and Switching exam covers IP and IP routing, non-IP desktop protocols such as IPX, and bridge- and switch-related technologies.

> **NOTE**   Sybex can help you pass the CCIE Routing and Switching exam with the *CCIE: Cisco Certified Internetworking Expert Study Guide,* Second Edition (ISBN 0-7821-4207-9).

CCIE Security (Exam 350-018)   The CCIE Security exam covers IP and IP routing as well as specific security components.

CCIE Voice (Exam 351-030)   The CCIE Voice exam covers those technologies and applications that make up a Cisco Enterprise VoIP solution.

Where Do You Take the Exam?

You can take the exams at any of the Sylvan Prometric or Virtual University Enterprises (VUE) testing centers around the world. For the location of a testing center near you, call Sylvan at (800) 755-3926 or VUE at (877) 404-3926. Outside of the United States and Canada, contact your local Sylvan Prometric Registration Center.

To register for a Cisco Certified Network Professional exam:

1. Determine the number of the exam you want to take. (The CIT exam number is 642-831.)

2. Register with the nearest Sylvan Prometric or VUE testing center. At this point, you will be asked to pay in advance for the exam. At the time of this writing, the exams are $125 each and must be taken within one year of payment. You can schedule exams up to six weeks in advance or as soon as one working day prior to the day you wish to take it. If something comes up and you need to cancel or reschedule your exam appointment, contact the testing center at least 24 hours in advance. Same-day registration isn't available for the Cisco tests.

3. When you schedule the exam, you'll get instructions regarding all appointment and cancellation procedures, the ID requirements, and information about the testing-center location.

Tips for Taking Your CCNP CIT Exam

The CCNP CIT test contains about 65 questions to be completed in about 90 minutes. However, understand that your test may vary somewhat from this estimate.

Many questions on the exam have answer choices that at first glance look identical—especially the syntax questions! Remember to read through the choices carefully, because "close" doesn't cut it. If you put commands in the wrong order or forget one measly character, your answer will be wrong. So, to practice, do the hands-on exercises at the end of the chapters over and over again until the solutions feel natural to you.

Unlike Microsoft or Novell tests, the exam has answer choices that are highly similar in syntax—although some syntax is dead wrong, it is usually just *subtly* wrong. Some other syntax choices may be right, but they're shown in the wrong order. Cisco does split hairs, and it is not at all averse to giving you classic trick questions. Here's an example:

```
access-list 101 deny ip any eq 23 denies Telnet access to all systems.
```

This statement looks correct to most people because they refer to the port number (23) and think, "Yes, that's the port used for Telnet." The catch is that you can't filter IP on port numbers (only TCP and UDP can be filtered in this way). Another indicator that this command is wrong is the use of an extended access list number but with any or no destination address for the destination.

> **NOTE** Cisco does have some simulation questions on the CIT exam. Make sure you've got hands-on skills to take this test. Practice with the hands-on labs in this book, and for further practice with routers and switches, check out the CCNP Virtual Lab from Sybex.

> **TIP** Also, never forget that the right answer is the Cisco answer. In many cases, more than one appropriate answer is presented, but the *correct* answer is the one that Cisco recommends.

Here are some general tips for exam success:

- Arrive early at the exam center, so you can relax and review your study materials.
- Read the questions *carefully*. Don't just jump to conclusions. Make sure that you're clear about *exactly* what each question asks.
- Don't leave any questions unanswered. They count against your score.
- When answering multiple-choice questions that you're not sure about, use the process of elimination to get rid of the obviously incorrect answers first. Doing this greatly improves your odds if you need to make an educated guess.
- As of this writing, the written exams still allow you to skip ahead and then return to previous questions. However, it is always best to check the Cisco website before taking any exam, to get the most up-to-date information.

After you complete an exam, you'll get immediate, online notification of your pass or fail status, a printed Examination Score Report that indicates your pass or fail status, and your exam results by section. (The test administrator will give you the printed score report.) Test scores are automatically forwarded to Cisco within five working days after you take the test, so you don't need to send your score to them.

What Does This Book Cover?

This book covers everything you need to pass the CCNP CIT exam. It teaches you how to document your network, and how to troubleshoot and maintain Cisco routers and switches in a large internetwork. Each chapter begins with a list of the topics covered, related to the CCNP CIT test, so make sure to read the list before working through the chapter.

- Chapter 1 discusses the complexity of today's internetworks and introduces you to the Cisco Troubleshooting Methodology. You'll study how to apply this methodology to network problems.

- Chapter 2 focuses on what goes into a network baseline, as well as how to create one. It also details two of the baseline's components: the network configuration table and the network topology diagram.

- Chapter 3 continues the discussion on documentation by explaining the end-system version of a network configuration table and network topology diagram. This chapter also takes you through the steps required to create these documents. In the second half of the chapter, various troubleshooting approaches are discussed and some end-system troubleshooting commands are reviewed.

- Chapter 4 reviews the OSI reference model and then discusses connection-oriented and connectionless protocols. Following this, the IP, ICMP, TCP, and UDP protocols are examined, and Layer 2 protocols are covered.

- Chapter 5 focuses on the skills and knowledge needed to use Cisco's built-in diagnostic tools in a TCP/IP environment. These tools include `show`, `debug`, and `logging` commands as well as a router core dump. This chapter also examines appropriate use of the ping and traceroute utilities. LAN and WAN problems are explored, and the chapter ends with a discussion of access lists.

- Chapter 6 is dedicated to covering IP routing protocols, specifically RIP, IGRP, EIGRP, OSPF, and BGP. The benefits and drawbacks of each are included, as well as the commands used to verify correct functionality. We also discuss the issues of redistributing these protocols.

- Chapter 7 examines serial and Frame Relay connectivity. You'll study the function of the `show` and `debug` IOS commands needed to successfully troubleshoot problems in serial and Frame Relay environments, as well as some common problem areas.

- Chapter 8 discusses ISDN and related protocols, specifically looking at what is necessary to set up an ISDN dial solution. In addition, time is spent looking at the `debug` output from the call setup, to show how an ISDN call is established.

- Chapter 9 details the functioning of Catalyst series switches. This chapter includes information on the architecture of the switch as well as the command syntax used to configure the switch. It also discusses the use of VLANs and trunking switch ports together.

- Chapter 10 is a summary chapter that takes the information from the previous chapters and applies it to real-world examples. These examples demonstrate combining the troubleshooting methodology with the technical skills learned in this book.

- The Glossary is a handy resource for Cisco vocabulary and is an excellent tool for understanding some of the more obscure terms used in this book.

Each chapter ends with review questions that are specifically designed to help you retain the knowledge presented. To really nail down your skills, read each question carefully.

How to Use This Book

This book can provide a solid foundation for the serious effort of preparing for the CCNP CIT exam. To best benefit from this book, use the following study method:

1. Take the Assessment Test immediately following this Introduction. (The answers are at the end of the test.) Carefully read over the explanations for any question you get wrong, and note which chapters the material comes from. This information will help you plan your study strategy.

2. Study each chapter carefully, making sure that you fully understand the information and the test topics listed at the beginning of each chapter. Pay extra-close attention to any chapter where you missed questions in the Assessment Test.

3. Note the questions that confuse you, and study those sections of the book again.

4. Before taking the exam, try your hand at the two bonus exams included on the CD that comes with this book. The questions in these exams appear only on the CD. This will give you a complete overview of what you can expect to see on the real thing.

5. Remember to use the products on the CD included with this book. The electronic flashcards and the EdgeTest exam-preparation software have all been specifically picked to help you study for and pass your exam. Study on the road with the *CCNP: Cisco Internetwork Troubleshooting Study Guide* eBook in PDF format, and test yourself with the electronic flashcards.

> The electronic flashcards can be used on your Windows computer, Pocket PC, or Palm device.

6. Make sure you review the Key Terms list at the end of each chapter. Appendix A includes all the commands used in the book, along with an explanation for each command.

To learn all the material covered in this book, you'll have to apply yourself regularly and with discipline. Try to set aside the same time every day to study, and select a comfortable and quiet place to do so. If you work hard, you'll be surprised at how quickly you learn this material. All the best!

What's On the CD?

We worked hard to provide some really valuable tools to help you with your certification process. All of these tools should be loaded on your workstation when studying for the test.

The Sybex Test Engine for Cisco CIT Test Preparation

New from Sybex, this test-preparation software prepares you to successfully pass the CIT exam. In the test engine, you'll find all the questions from the book, plus the two additional Bonus Exams that appear exclusively on the CD. You can take the Assessment Test, test yourself by chapter, or take the two Bonus Exams that appear on the CD.

Electronic Flashcards for PC, Pocket PC, and Palm Devices

After you read the *CCNP: Cisco Internetwork Troubleshooting Study Guide*, you'll of course read the review questions at the end of each chapter and study the practice exams included in the book and on the CD. But wait, there's more! Test yourself with the flashcards included on the CD. If you can get through these difficult questions and understand the answers, you'll know you'll be ready for the CCNP CIT exam.

The flashcards include 150 questions specifically written to hit you hard and make sure you are ready for the exam. Between the review questions, practice exam, and flashcards, you'll be more than prepared for the exam.

CCNP: Cisco Internetwork Troubleshooting Study Guide in PDF

Sybex offers this Cisco Certification book on the accompanying CD so that you can read the book on your PC or laptop. The eBook is in Adobe Acrobat format, and Acrobat Reader is included on the CD as well. This is extremely helpful to readers who travel and don't want to carry a book, as well as to readers who find it more comfortable reading from their computer.

How to Contact the Authors

You can reach Art Pfund by e-mailing him at `art.pfund@comcast.net`.

Assessment Test

1. Which are reasons for using a troubleshooting method? (Choose all that apply.)
   A. Problem isolation and resolution will occur more quickly.
   B. No documentation needs to be done when following a method.
   C. Due to complex topologies and technologies, a systematic method is the most efficient way to resolve network problems.
   D. All of the above.

2. What are the benefits of gathering additional facts for troubleshooting? (Choose all that apply.)
   A. Possible causes of problems may be identified.
   B. A specific problem definition may be created.
   C. Information is provided for a baseline.
   D. All of the above.

3. Which of the following are key components of creating an action plan? (Choose all that apply.)
   A. Multiple changes as long as they are documented
   B. Changes that do not compromise security
   C. Changes that have only brief network impact
   D. Back-out plans

4. How many methods of problem isolation exist?
   A. 2
   B. 3
   C. 4
   D. 6

5. Which of the following steps are part of the Cisco troubleshooting methodology? (Choose all that apply.)
   A. Observation of results
   B. Observation of changes
   C. Iteration
   D. Documentation
   E. Problem definition
   F. Problem resolution
   G. Troubleshooting

6. Which protocol attributes are associated with the Internet Protocol (IP)? (Choose all that apply.)

    A. Connection-oriented

    B. Connectionless

    C. Layer 2

    D. Layer 3

7. Select the potential attributes of a connectionless protocol.

    A. Broadcast control

    B. Sequenced PDUs

    C. Broadcast transmissions

    D. Wireless connectivity

8. Choose all protocols that operate only at Layer 3 from the following list:

    A. PPP (Point-to-Point Protocol)

    B. IP (Internet Protocol)

    C. EIGRP (Enhanced Interior Gateway Routing Protocol)

    D. SDLC (Synchronous Data Link Control)

    E. X.25

    F. BGP (Border Gateway Protocol)

9. Choose all the Layer 2 protocols from the following list:

    A. TCP

    B. Ethernet

    C. UDP

    D. IP

    E. Token Ring

    F. FDDI

    G. EIGRP

10. Choose two attributes that a connection-oriented protocol possesses.

    A. Flow control

    B. Error control

    C. Broadcast control

    D. Collision detection

11. Which of the following are parts of a network baseline? (Choose all that apply.)

    A. End-system network configuration table

    B. Network overview document

    C. Network summary document

    D. Network topology diagram

12. What Windows 2000 command shows all the IP addresses and TCP port numbers of the current connections to an end-system?

    A. `netstat`

    B. `ipconfig`

    C. `ifconfig`

    D. `route`

13. What is SNMP used for?

    A. Creating network maps

    B. Traffic analysis

    C. Statistical/environmental data collection

    D. All of the above

14. A network configuration table usually contains what kind of information?

    A. IP addresses

    B. CRCs

    C. Interface name

    D. SNMP configuration

    E. `show running-config`

    F. Interface type

    G. Interface speed

    H. VLANs

15. You are seeing incrementing interface resets on an interface. What is the most appropriate troubleshooting method to use for this situation?

    A. Bottom-up troubleshooting

    B. Top-down troubleshooting

    C. Divide-and-conquer troubleshooting

    D. Wait-and-see troubleshooting

16. What Unix command shows the IP address and subnet mask of the interface?

    A. `ipconfig`

    B. `ifconfig`

    C. `cat /etc/resolv.conf`

    D. `netstat`

17. Which of the following routing protocols is a distance vector protocol and a Cisco proprietary routing protocol?

    A. EIGRP

    B. IGRP

    C. RIP

    D. BG

18. Which commands should be used in conjunction for thorough problem isolation? (Choose two.)

    A. `ping`

    B. `show ip interface`

    C. `traceroute`

    D. `arp`

19. What command(s) can be issued on a Windows XP system to provide interface IP information?

    A. `show ip interface`

    B. `ipconfig /all`

    C. `winipcfg`

    D. `ipcfg`

20. Which protocols are used for dynamic IP address assignment? (Choose two.)

    A. AutoIP

    B. AutoARP/IP

    C. BootP

    D. DHCP

21. Choose the troubleshooting tool that is used to test for reachability and connectivity.

    A. `Traceroute`

    B. Debug

    C. `show interface`

    D. Ping

22. How many levels of `ping` and `traceroute` are there on Cisco routers?

   A. One

   B. Two

   C. Three

   D. Four

23. From the following list, choose the troubleshooting tool that is used for testing the path from a source host to a destination host.

   A. Traceroute

   B. Debug

   C. `show interface`

   D. Ping

24. When is a "default gateway" used on the router?

   A. When a packet leaves the router

   B. When no route exists in the route table

   C. When a static route has been set

   D. Only when the router is in boot mode

25. Why is a default metric setting necessary for route redistribution?

   A. It isn't necessary.

   B. The routes being injected must be assigned metrics that the parent protocol understands.

   C. A default metric setting provides better metrics when performing route redistribution.

   D. A default metric setting converts the parent protocol's metric to match the protocol being redistributed.

26. Which LMI (Local Management Interface) type is on by default on a Cisco router?

   A. LMI

   B. Cisco

   C. ANSI

   D. ITU-T

   E. IETF

27. What are the valid LMI types? (Choose all that apply.)

   A. LMI

   B. Cisco

   C. ITU-T

   D. ANSI

28. What are the valid Frame Relay encapsulation types? (Choose all that apply.)

    A. IETF

    B. ITU-T

    C. Cisco

    D. ANSI

29. Which kind of encapsulation is used by default on Cisco serial interfaces?

    A. SDLC

    B. PPP

    C. HDLC

    D. X.25

30. What type of tests are useful in testing for end-to-end serial link integrity?

    A. Ping

    B. Traceroute

    C. Loopback

    D. Loopup

31. Which channel is used by q.931 and q.921 for communication?

    A. A channel

    B. B channel

    C. D channel

    D. Both B and D channels

32. Which ISDN protocol is used for Layer 3 connection setup?

    A. CHAP

    B. PPP

    C. q.921

    D. q.931

33. Which command should be used to display the connection setup for Layer 3?

    A. `show interface bri n`

    B. `debug isdn q931`

    C. `debug interface bri`

    D. `debug isdn q92`

34. Which ISDN protocol is used for Layer 2 connection setup?

   A. CHAP

   B. PPP

   C. q.921

   D. q.931

35. Which channel does PPP use when negotiating the connection?

   A. A channel

   B. B channel

   C. D channel

   D. Both B and D channels

36. Which of the following are characteristic of extended IP access lists? (Choose all that apply.)

   A. Can be used to limit debug output

   B. Can be used to filter Layer 2 frames

   C. Can be applied to ports on a switch

   D. Filter on the TCP or UDP port

37. What does a result of P mean in the output of a `ping` command?

   A. Destination Unreachable

   B. Source Quench

   C. Protocol Unreachable

   D. Network Unreachable

   E. Unable to Fragment

38. Which of the following command outputs would most likely indicate a problem at the Data-Link layer?

   A. Serial 2/3 is up, line protocol is down

   B. Serial 2/3 is up, line protocol is up

   C. Serial 2/3 is down, line protocol is down

   D. Serial 2/3 is down, line protocol is up

39. Which of the following are guidelines for creating network documentation? (Choose all that apply.)

   A. Determine the scope.

   B. Document everything.

   C. Put as much information as possible on network documents.

   D. Keep documents accessible.

40. What command is used for displaying information about Cisco routers that are connected to a switch?

  A. `show connections`

  B. `show vtp neighbor`

  C. `show ip route`

  D. `show cdp neighbor`

41. What command on a Windows NT end-system is used to add routes to that end-system?

  A. `route add`

  B. `ip add route`

  C. `ip route add`

  D. `add route`

42. What are some of the benefits of a named access list over a numbered access list? (Choose all that apply.)

  A. A named access list can be applied to all interface types.

  B. Individual lines can be removed from a named access list.

  C. Named access lists are easier for the router to work with.

  D. Named access lists are easier for the network administrator to work with.

43. Which of these commands will verify whether an https web server, 10.7.7.7, was reachable through the network?

  A. `debug https traffic`

  B. `telnet 10.7.7.7`

  C. `telnet 10.7.7.7 80`

  D. `telnet 10.7.7.7 443`

44. You are troubleshooting a serial connection problem. After making a couple of changes, you find that the problem is still occurring. What should your next step be?

  A. Continue making changes.

  B. Back out the changes you've made up to this point and begin gathering facts again.

  C. Reload the router.

  D. Execute a `shut/no shut` on the interface.

45. How often should the network configuration table be updated?

  A. There is no such document.

  B. Once a week.

  C. Once a month.

  D. Once a year

  E. Anytime there is a change in the network.

46. What are the three major roles of a router when configured with VLANs?

   A. Define the collision domain.

   B. Provide Layer 2 VLAN switching.

   C. Provide Layer 2 VLAN translation.

   D. Provide Layer 3 VLAN routing.

47. Which of the following VLAN encapsulation types do Cisco routers support? (Choose all that apply.)

   A. Inter-Switch Link (ISL)

   B. IEEE Ethernet 802.3

   C. IEEE 802.1Q

   D. IEEE 802.1Z

48. When using a router, which of the following scenarios will not work?

   A. VLAN 10 uses ISL while VLAN 20 uses 802.1q.

   B. The switch is configured to use ISL and the router uses 802.1q.

   C. VLAN 10 uses 802.1q, then tries to communicate with a remote host not on a VLAN.

   D. Both VLAN 10 and VLAN 20 use 802.1q.

49. What switch command shows VTP state information on the switch?

   A. `show vtp state`

   B. `show vtp`

   C. `show vtp domain`

   D. `show vtp status`

50. What does the term "blocking" mean with regard to a Catalyst port?

   A. An access list has been applied to the port.

   B. Packets are not allowed out of the port.

   C. Spanning tree has blocked the port to prevent a loop.

   D. The port has been shut down.

51. What router command will show the IP listing of the helper addresses applied on an interface?

   A. `show interface`

   B. `show ip interface`

   C. `show interface helper`

   D. `show helper brief`

52. After a "forklift" upgrade has been performed on a server in which the old hardware was removed and a new server put in its place, you find that the new server cannot be pinged from the directly connected subnet. The new server was given the IP address of the old server, and it has been verified that the new server is configured correctly. What could be the cause of the problem?

A. Access list needs to be updated.

B. Routing table on the router needs to be cleared to flush out the old entry.

C. ARP table on the router needs to be cleared to flush out the old entry.

D. A static route must be added to the router.

53. Which of the following are information items that will be requested when you open a TAC case? (Choose all that apply.)

A. Output from a show tech-support

B. Support contract number

C. Mailing address

D. Software versions

54. Which 6500 card provides Layer 3 capabilities to the 6500 switch?

A. RSM

B. RFSC

C. MSFC

D. PFC

55. Which command would you use to verify network connectivity to an end-system?

A. arp

B. tracert

C. traceroute

D. ping

56. What do the following lines of router output indicate? (Choose all that apply.)

```
Router_C#show int ethernet 0/1
Ethernet0/1 is up, line protocol is up
  Hardware is Lance, address is 0000.0c47.abea (bia
    0000.0c47.abea)
  Internet address is 172.16.60.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255,
    load 46/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
 ARP type: ARPA, ARP Timeout 04:00:00
```

A. The interface is up and appears to be functioning properly.

B. This interface is in loopback.

C. The encapsulation type for this interface is ARPA.

D. The bandwidth metric for this interface is 100Mbps.

57. Which configuration register setting will cause the router to boot the IOS image from the boot ROM?

   A. 0x2000

   B. 0x2101

   C. 0x1002

   D. 0x2102

58. What do the following lines of router output indicate? (Choose all that apply.)

```
Router_A#show interface to0
... some output deleted ...
  MTU 4464 bytes, BW 16000 Kbit, DLY 630 usec, rely 255/255,    load 1/255
  Encapsulation SNAP, loopback not set, keepalive set (10 sec)
  ARP type: SNAP, ARP Timeout 04:00:00
  Ring speed: 16 Mbps
... output removed ...
  Last clearing of "show interface" counters never
```

   A. The ring speed is 4Mbps.

   B. The ring speed is 16Mbps.

   C. The interface counters have never been cleared.

   D. Encapsulation is SNMP.

59. Look at the following outputs from two different interfaces connected to each other. Why aren't the interfaces functioning properly?

```
Router_A#show interface to0
TokenRing0 is up, line protocol is down
  Hardware is TMS380, address is 0007.787c.e14b (bia    0007.787c.e14b)
  Internet address is 172.16.30.1, subnet mask is    255.255.255.0
  MTU 4464 bytes, BW 16000 Kbit, DLY 630 usec, rely 255/255,    load 1/255
  Encapsulation SNAP, loopback not set, keepalive set (10 sec)
  ARP type: SNAP, ARP Timeout 04:00:00
  Ring speed: 16 Mbps
  Single ring node, Source Route Transparent Bridge capable
  Ethernet Transit OUI: 0x000000
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
```

```
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored,        0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 output buffer failures, 0 output buffers swapped out
        5 transitions
Router_B#show interface to1
TokenRing0 is up, line protocol is down
   Hardware is TMS380, address is 0007.787c.e14b (bia     0007.787c.e14b)
   Internet address is 172.16.30.2, subnet mask is     255.255.255.0
   MTU 4464 bytes, BW 4000 Kbit, DLY 630 usec, rely 255/255,    load 1/255
   Encapsulation SNAP, loopback not set, keepalive set (10 sec)
   ARP type: SNAP, ARP Timeout 04:00:00
   Ring speed: 4 Mbps
   Single ring node, Source Route Transparent Bridge capable
   Ethernet Transit OUI: 0x000000
   Last input never, output never, output hang never
   Last clearing of "show interface" counters never
   Queueing strategy: fifo
   Output queue 0/40, 0 drops; input queue 0/75, 0 drops
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
      0 packets input, 0 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun,   0 ignored,        0 abort
      0 packets output, 0 bytes, 0 underruns
      0 output errors, 0 collisions, 0 interface resets
      0 output buffer failures, 0 output buffers swapped out
      5 transitions
```

    A. Duplicate IP addresses

    B. Lobe wire fault

    C. Ring speed mismatch

    D. Five carrier transitions

60. Which of the following factors may contribute to excessive collisions on an Ethernet interface? (Choose all that apply.)

    A. Ethernet interface

    B. Transceiver

    C. Cable

    D. Encapsulation

Answers to Assessment Test

1. C.   Quick resolution of problems is not guaranteed by using a model, and documentation should always be performed. For further explanation of the reasons for using a troubleshooting method, refer to Chapter 1.

2. A, B.   A baseline contains information taken from a normally functioning network, so gathering baseline information is not part of troubleshooting. The benefits of gathering additional facts for troubleshooting are that you identify possible causes of trouble, and that you have information to contribute to the problem definition. For further explanation of gathering facts for troubleshooting, refer to Chapter 1.

3. B, D.   Making multiple changes creates more difficulty when you have to back out of changes, and multiple changes do not allow for good observation results. Changes should not create any adverse network impact. For further explanation of creating an action plan, refer to Chapter 1.

4. B.   The three methods for isolating the source of a network problem are outside-in, inside-out, and divide-by-half. For further explanation of methods of problem isolation, refer to Chapter 1.

5. A, C, E.   In addition to observation of results, iteration, and problem definition, Cisco's troubleshooting method contains other steps not included in this question. Though not an official step in the process, documenting changes after they are complete is an important part of the overall process. For further explanation of Cisco's troubleshooting method, refer to Chapter 1.

6. B, D.   IP is a connectionless protocol and a Layer 3 protocol. For further information about IP, refer to Chapter 4.

7. C.   Connectionless protocols do not use any type of control. Sequenced PDUs are a type of control. Physical connectivity does not determine the protocol properties. For further information about connectionless protocols, refer to Chapter 4.

8. B, C, F.   IP, EIGRP, and BGP are Layer 3; PPP, SDLC, and X.25 all operate at Layer 2. Refer to Chapter 4 for further information.

9. B, E, F.   Ethernet, token Ring and FDDI are all Layer 2 technologies. For further information, refer to Chapter 4.

10. A, B.   Flow control and error control allow for complete connection and data-transfer control. For further information about connection-oriented protocols, refer to Chapter 4.

11. A, D.   The network baesline consists of network configuration tables, the network topology diagram, end-system network configuration tables and end-system topology diagrams. For additional information, refer to Chapter 2.

12. A.   The `netstat` command gives you the IP addresses and TCP port numbers of the current connections to an end-system, for both Windows- and UNIX-based systems. For further information, refer to Chapter 3.

13. C.   Simple Network Management Protocol (SNMP) is used to collect statistical/environmental data from network devices. For additional information on SNMP, refer to Chapter 4.

14. A, C, F, G, H.   The network configuration table holds fundamental information about the configuration of the network. Some of the standard items included in this table are device name, flash statistics, DRAM, IOS/CATOS, interface number, MAC address, speed, duplex, VLANs, trunking, IP address, subnet, subnet mask, and routing protocol. For details about the network configuration table, refer to Chapter 2.

15. A.   Interface resets are usually indicative of a physical issue in the network. Therefore, the bottom-up approach is the most appropriate. For details, refer to Chapter 3.

16. B.   The `ifconfig -a` command will show information regarding Unix interface configuration. Refer to Chapter 3 for details.

17. B.   Both EIGRP and IGRP are proprietary routing protocols, but EIGRP is a hybrid routing protocol and not a distance vector routing protocol like IGRP. Refer to Chapter 6 for more information.

18. A, C.   Using both ping and traceroute in conjunction greatly aids problem isolation. Refer to Chapter 5 for more information.

19. B.   The `ipconfig /all` command can be used on a Windows XP machine; `show ip interface` is for use on a router; `winipcfc` is used on Windows 9x and ME; and `ipcfc` is incorrect syntax. Refer to Chapter 3 for more information on these commands.

20. C, D.   BootP and DHCP (Dynamic Host Configuration Protocol) are used for IP address assignment. (The other two answers, AutoIP and AutoARP/IP, don't exist.) Refer to Chapter 5 for more information.

21. D.   Ping uses ICMP (Internet Control Message Protocol) to test for connectivity of remote hosts. Refer to Chapter 5 for more details.

22. B.   There are two levels, user and privileged. Refer to Chapter 5 for more details.

23. A.   Traceroute tests the route or path from a source to a destination. Refer to Chapter 5 for more information.

24. B.   The term "default" indicates that no other route has been specified. So instead of dropping the packet, the router forwards it out the default gateway. Refer to Chapter 6 for more information.

25. B.   Routes from the incoming protocol must be assigned new metrics so they can be redistributed. Refer to Chapter 6 for more information.

26. B.   Cisco LMI is on by default. Refer to Chapter 7 for more information.

27. B, C, D.   Valid LMI types are Cisco, ITU-T, and ANSI. LMI stands for Local Management Interface. Refer to Chapter 7 for more information.

28. A, C.   There are only two valid encapsulation types for Frame Relay: IETF and Cisco. Refer to Chapter 7 for more information.

29. C.   HDLC is an enhancement over SDLC, and PPP is a protocol, not an encapsulation. X.25 is not configured by default. Refer to Chapter 7 for more information.

30. C.   Loopback tests can test for link integrity without any additional protocols such as PPP, IP, or others. Refer to Chapter 7 for more details.

31. C.   The q.931 and q.921 protocols use the D channel for information signaling. Refer to Chapter 8 for more information.

32. D.   CHAP (Challenge Handshake Authentication Protocol) and PPP (Point-to-Point Protocol) are not specific to ISDN and q.921 is used for Layer 2 setup. Refer to Chapter 8 for more information.

33. B.   The `debug isdn q931` command displays all steps of the connection sequence. Refer to Chapter 8 for more information.

34. C.   The q.921 protocol is used for Layer 2 connection setup. CHAP (Challenge Handshake Authentication Protocol) and PPP (Point-to-Point protocol) are not specific to ISDN, and q.931 is used for Layer 3 setup. Refer to Chapter 8 for more information.

35. B.   Since data (payload) is going to be from point to point, the PPP (Point-to-Point protocol) link must be set up between the local and remote TE (Terminal Equipment) on the B channel. Refer to Chapter 8 for more information.

36. A, D.   Extended access lists can be used to limit debug output and can filter based on UDP or TCP port numbers. Refer to Chapter 5 for details.

37. C.   The P output from the `ping` command indicates that the protocol was unreachable. Refer to Chapter 5 for more information about `ping`.

38. A.   If the interface is up but the line protocol is down, there is most likely a problem at Layer 2, the Data-Link layer. Refer to Chapter 5 for more detail.

39. A, D.   The five keys to good network documentation are as follows: Determine the scope, know your objective, be consistent, keep documents accessible, and maintain the documentation. Refer to Chapter 2 for more information about documentation.

40. D.   The `show cdp neighbor` command provides information regarding any Cisco device, including routers, connected to a switch. Refer to Chapter 10 for more information.

41. A.   `route add` is the correct syntax for the command to add routes to a Windows NT end-system. Refer to Chapter 3 for more information.

42. B,D.   Named access lists allow for the removal of individual lines, whereas numbered access lists are removed entirely when the `no` command is issued. In addition, because their names can be descriptive, named access lists are easier for network administrators to work with. For the router, named access lists are no harder or easier to work with router. Refer to Chapter 5 for more information.

43. D.   This command will telnet to the server on port 443. If a connection is made (though no meaningful data will be sent), then the path through the network on port 443 is functioning correctly. Refer to Chapter 3 for more information.

44. B.   If the original set of changes does not correct the problem, then these should be backed out and the troubleshooting procedure repeated. Refer to Chapter 1 for more information.

45. E.   All network documentation should be updated whenever there is a change in the network. Refer to Chapter 2 for more information.

46. B, C, D.   In addition to switching and translation at Layer 2, and routing at Layer 3, a router configured with VLANs provides other roles in a switched network. The collision domain is defined by the switch port, not the router. Refer to Chapter 9 for more information on this subject.

47. A, C.   Cisco routers support both ISL and 802.1Q. Refer to Chapter 9 for more information.

48. B.   The router and switch must use the same encapsulation across the connection. Other interfaces do not matter. Refer to Chapter 9 for more information.

49. C.   The correct syntax for the switch command to show VTP state is `show vtp domain`. Refer to Chapter 9 for more information.

50. C.   Blocking is a step or state in the Spanning-Tree Protocol that prevents loops. Refer to Chapter 9 for more information.

51. B.   The `show ip interface` command provides a list of helper addresses on an interface. Refer to Chapter 5 for more information.

52. C.   Of the answer options listed, the most likely cause of the new server not responding to a ping from the subnet is that the ARP table in the router still has an entry for the server associated with the old server's MAC address. Refer to Chapter 5 for more information.

53. A, B, D.   In addition to `show tech-support` output, the support contract number, and software version information, you need to have network topology information and a problem description. Refer to Chapter 10 for more information.

54. C.   The Multilayer Switching Feature Card (MSFC) provides routing capabilities for the 6500. Refer to Chapter 9 for more information.

55. B.   A `ping` is the simplest and best way to test network connectivity between two devices. Although a `traceroute` command will work, this is not its primary function. Refer to Chapter 5 for additional information.

56. A, C.   This output tells you that the interface is not in loopback and the bandwidth metric is only 10Mbps. Refer to Chapter 10 for more information.

57. B.   0x2101 is the correct configuration register setting for a router to enter boot mode. Refer to Chapter 10 for more details about configuration register settings.

58. B, C.   The ring speed is indicated by the `Ring speed: 16 Mbps` output, and the clearing of the counters is indicated by the `Last clearing of "show interface" counters never` output. The encapsulation is SNAP, as indicated by the `Encapsulation SNAP` output. Refer to Chapter 10 for more information.

59. C.   The carrier transitions could be caused by the ring speed mismatch. Refer to Chapter 10 for more information.

60. A, B, C.   Collisions can be caused by any piece of hardware involved in an Ethernet connection. Refer to Chapter 10 for more information about collisions.

Chapter

1

Troubleshooting Methodology

EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

✓ **Know troubleshooting methodologies.**

Troubleshooting is a skill that takes time and experience to fully develop. To be successful when diagnosing and repairing network failures, a good set of troubleshooting tools and skills is essential.

While there's no specific exam objective that maps to this chapter, the information presented here is nevertheless important to the exam. This chapter emphasizes the importance of following a specific set of troubleshooting steps when you try to diagnose and solve network problems. An effective troubleshooting methodology is needed because of the complexity of today's network environments. As a Cisco Certified Network Professional, you need to understand and know how to apply an efficient and systematic troubleshooting methodology. Otherwise, you would be required to have a very intimate understanding of the network you are troubleshooting. It is imperative that you learn troubleshooting skills and understand the information available to you while solving network problems.

The Complexity of Internetworks

When a network failure occurs, time is of the essence. When a production network goes down, several things are affected. The most important of these is the bottom line—network failures cost money. A good example is a call-center network. The company relies on the network to be available for its employees so that they can take phone orders, answer inquiries, or perform other business transactions that generate income. A failure in this environment needs to be diagnosed and repaired in a timely manner. The longer the network is down, the more money the company loses.

To minimize monetary and productivity losses, network failures must be resolved quickly. Troubleshooting is an integral part of getting this done. Intimate knowledge of a network also facilitates rapid resolution. Armed with a few troubleshooting skills and intimate knowledge of the network, you can solve most problems rather quickly, thus saving money.

Hold on a minute. What if you're new on the job and you don't yet have an intimate knowledge of the network? You can probably get up to speed quickly enough, right? Although that may have been the case in the past, getting up to speed becomes an overwhelming challenge in today's complex networks. These networks consist of many facets of routing, dial-up, switching, video, WAN (ISDN, Frame Relay, ATM, and others), LAN, and VLAN technologies. Refer to Figure 1.1 to get an idea of how these technologies intertwine. Notice that ATM, Frame Relay, Token Ring, Ethernet, and FDDI all are present. Each technology has its own properties and commands to allow for troubleshooting. Various protocols are used for each of these technologies. In addition, different applications require specific network resources. (At least the

seven-layer OSI model, which you will review in Chapter 4, is used to maintain a common template when designing new technologies and protocols.) It would take you a long time to master all of the technologies implemented in the network and to be able to solve network problems, based on your knowledge of the network alone. All of these factors contribute to today's complex network environments.

There must be an easier, more logical way to efficiently and successfully troubleshoot without having to become intimately familiar with every network environment. Well, you'll be happy to know that there is an easier option—following a troubleshooting model—and it is discussed in detail in this chapter. By following a troubleshooting model, the need for intimate knowledge of the network is reduced. A troubleshooting model should be adopted to help resolve network malfunctions and reduce downtime.

Let's move on to discuss Cisco's model in detail.

FIGURE 1.1   Today's complex enterprise network
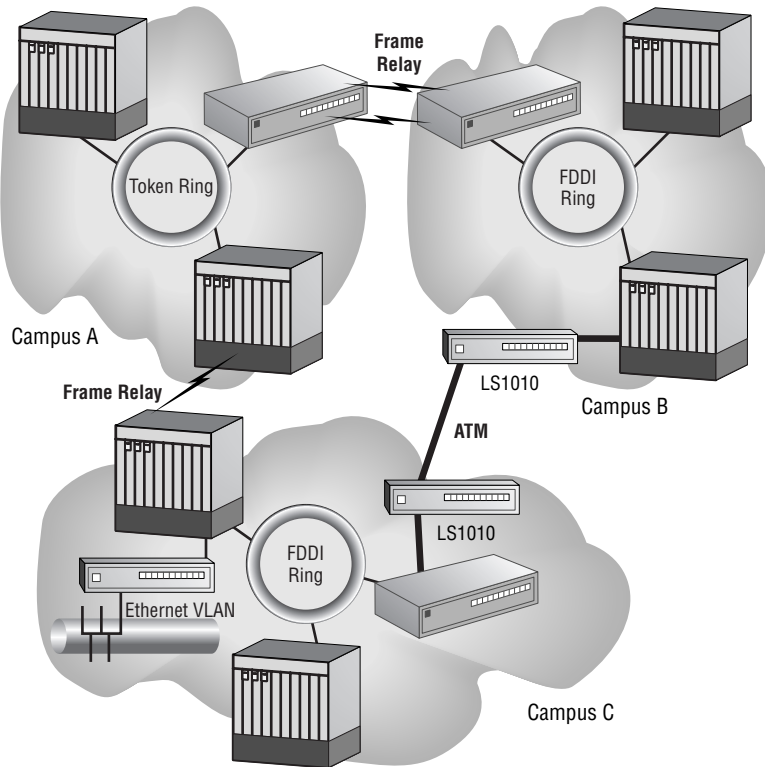
The Problem-Solving Model

Imagine trying to solve a network failure by using a different approach every time. With today's complex networks, the possible scenarios would be innumerable. Because so many different things can go wrong within a network, it would be possible to start from many different points. Not only is this an ineffective method of troubleshooting, but it is also time-consuming, and time is very valuable in a "network down" situation.

Cisco has designed an effective *troubleshooting model* that contains seven steps. A troubleshooting model is a list of troubleshooting steps or processes that can be followed to provide an efficient manner of resolving network problems. The headings in this section contain information specific to each step of the troubleshooting model. (Steps 4 and 5 are combined into one section of the chapter—creating and implementing the action plan.) After the seven steps are completed and the problem is resolved, a few more actions follow, such as completing documentation of the problem-solving events.

To be effective when troubleshooting and to achieve faster resolution times, follow the model outlined in Figure 1.2. This flow chart shows the seven steps.

The process begins when a network failure is reported to you. Following are brief descriptions of the steps to take:

1. Define the problem.   At this point in the process it is important to make a determination of the issue, identifying sets of symptoms and potential causes.

F I G U R E   1 . 2   Cisco's troubleshooting model
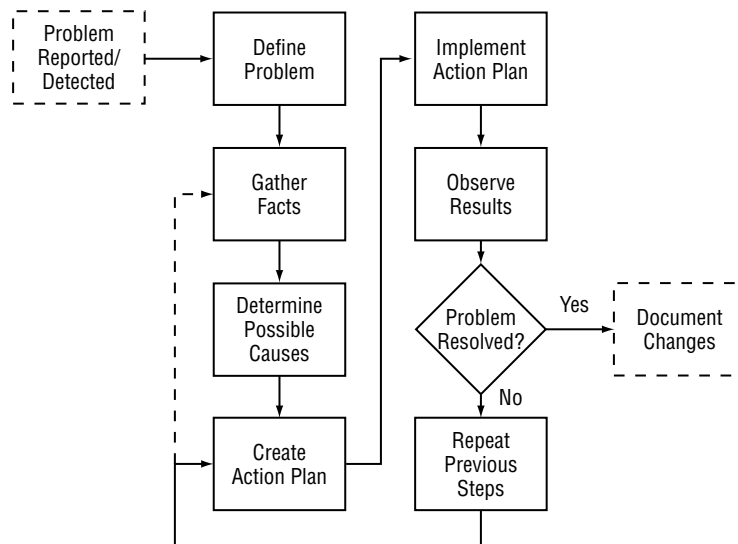
2. Gather detailed information. These facts about the problem can be obtained from a number of sources, including key users, network management systems, output from router and switch diagnostic commands, and protocol analyzer traces.

3. Consider possible scenarios. Brainstorm and come up with several possible or probable causes of the failure. Also, when developing this list, eliminate items that are definitely not the cause of the problem.

4. Create an action plan. Begin with the most likely source of the trouble and devise a plan to correct this issue, changing only one variable at a time. If you change multiple items simultaneously, it is possible that the problem will be resolved without your identifying the root cause. This then leaves the potential for the problem to repeat itself in the future.

5. Implement the action plan. As you implement each step of the action plan, carefully check to see if the problem has been resolved.

F I G U R E 1 . 3 Example campus network
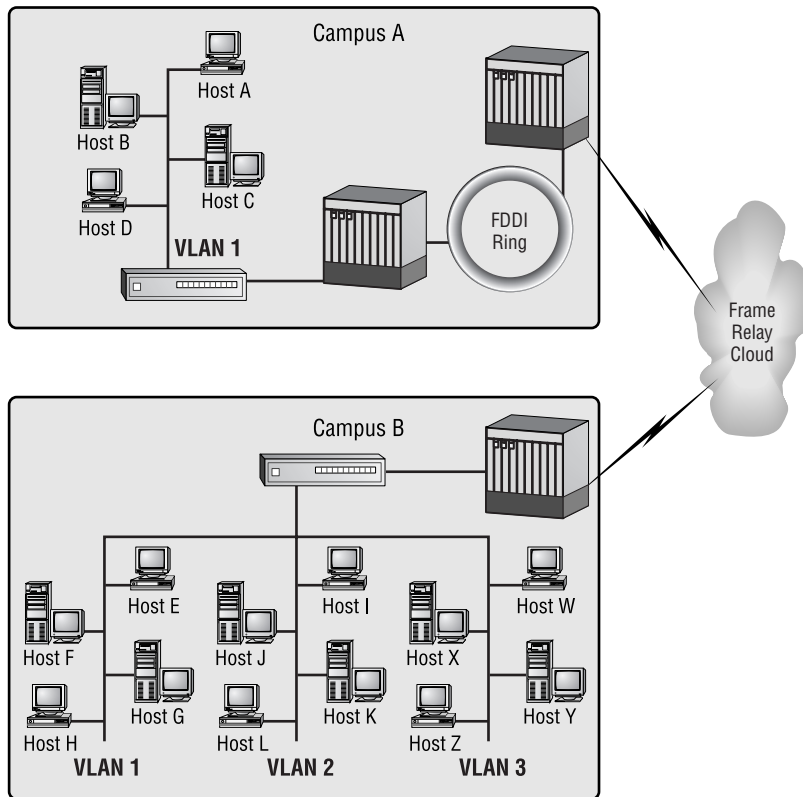
6. Observe the results of implementing the action plan.   In many instances it will be clear when the problem is resolved; however, in those cases where the problem is subtler, a more structured observation technique must be used. This technique involves many of the same tools used in the fact-gathering portion of the process, such as talking to users, employing network management tools, and checking router and switch output.

7. Repeat the process if the action plan doesn't fix the problem.   Revise your action plan to address the next most likely source of the trouble. Be sure to undo the changes that were attempted in the previous attempt. Then repeat the process starting with step 4. If there are no more potential causes for which to create an action plan, start with step 2 and repeat the process.

The best way to understand how Cisco's model works and how you should use it is by looking at an example. For this example, assume you are in charge of operational support of the network pictured in Figure 1.3. There are two campus networks, connected via a Frame Relay cloud. Within each network, VLANs are connected to a Catalyst 6500 switch and then to a core router that has a connection to the Frame Relay cloud in one way or another.

The fun begins when you get a call from a user who "can't get to Host Z." Based on this information, let's apply Cisco's troubleshooting model to solve the user's difficulty and fix the problem in the network.

Step 1: Define the Problem

As you can see, the user's problem is vague; you need more information if you are to solve the problem any time soon. This is where *problem definition* comes in. Problem definition is the step in the troubleshooting model when details are used to define what the most likely cause of a problem is. Now, while you still have the user on the line, the first step is to ask him what he means when he says he can't "get to" Host Z. The user then defines the situation by telling you that he can't FTP to Host Z. Ask the user if he experiences any other difficulties or if this is the only one. Verify where the user is currently located. After these preliminary questions, you'll have a basic idea of what is and isn't working. Unfortunately, you can't simply assume that the FTP is broken, because there are many other pieces of the network that can contribute to this problem.

It is also important to realize that you may want or need to gather facts before you actually form your problem statement. By gathering facts to help define the issue, the diagnosis of the problem or problems will be more accurate and will help you solve the trouble more quickly in the end. Problem definition and fact gathering should be used in tandem for a quick and accurate resolution.

Once you have enough information to define the problem, you should create a problem statement that is specific, concise, and an accurate description of what needs to be solved. In this case, you might have a statement that says *User A from Campus A cannot FTP to Host Z on Campus B*. With a good statement of the problem, it is easier to focus on the problem itself and not try to troubleshoot issues that do not fall within the problem definition.

Step back for a moment before you actually form your final problem statement. You need to gather more information before you can form an accurate problem statement. It's time to move on to the fact-gathering step. Keep in mind, however, that after you accumulate all the information, you have to come back and create your problem statement.

Step 2: Gather Facts

At this point, the problem is still pretty vague and needs more definition. This is where the fact-gathering step of the troubleshooting model is employed. *Fact gathering* is the process of using diagnostic tools to collect information specific to the network and network devices that are involved in a problem. Additional information should include data that excludes other possibilities and helps pinpoint the actual problem. An example of fact gathering in the case we're discussing is to verify whether you can ping, Traceroute, or Telnet to Host Z, thus reducing the number of possible causes.

Depending on the user and situation, you may or may not be able to get more detailed information. It is up to you as a network engineer or administrator to solve the problem, which means that you may have to get the information yourself.

It is important that you gain as much information as possible to actually define the problem while in the problem-definition phase of the troubleshooting model. Without a proper and specific definition of the problem, it will be much harder to isolate and resolve. Information that is useful for defining a problem is listed in Table 1.1.

T A B L E   1 . 1   Useful Information for Defining a Problem

Information	Example
Symptoms	Can't Telnet, FTP, or get to the WWW.
Reproducibility	Is this a one-time occurrence, or does it always happen?
Timeline	When did it start? How long did it last? How often does it occur? Has the current configuration ever worked properly?
Scope	What are you able to access successfully via Telnet or FTP? Which WWW sites can you reach, if any? Who else does this affect?
Baseline Info	Were any recent changes made to the network configurations?

All of this information can be used to guide you to the actual problem and to create the problem statement. Use your network topology diagram and check each item in Table 1.1.

Identify Symptoms

First, you need to define what is working and what isn't. You can do this by identifying the symptom and defining the scope. Figure 1.4 is a picture of your network. Although the large X on the Frame Relay cloud represents that there is an FTP connectivity issue, it does not indicate the location of the failure. Right now, all you know is that a single user could not FTP to Host Z.

F I G U R E   1 . 4   Host A cannot FTP to Host Z.
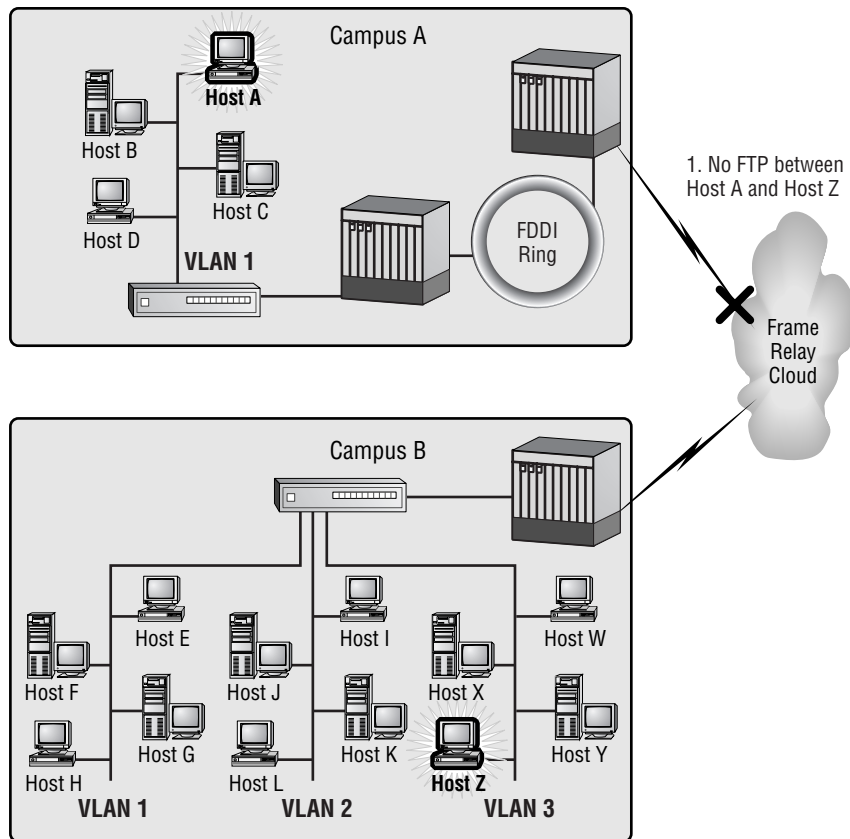
Reproduce the Problem

Before spending time and effort trying to solve this problem, verify that it is still a problem. Troubleshooting is a waste of time and resources if the problem can't be reproduced. It's just like a dog chasing its tail. If the issue is intermittent, further steps should be taken to capture as much information as possible about the event the next time it does occur. This will help narrow down the scope of items you will look at.

Understand the Timeline

In addition to verifying whether the problem is reproducible, it is important to investigate the frequency of the problem. For instance, maybe it happens only once or twice a day. By establishing a timeframe you can more readily identify any possible causes. In addition, you need to know whether this is the first time the user has attempted this function. There is a different set of variables involved with an item that worked yesterday but not today than there is with something that fails during first-time use. Obviously, if it worked yesterday, you can look at what changed overnight as well as looking for something that is broken. If the user has never used this

feature before, there may be an existing access list or other security device that has only now been activated by the user's initial use of this application.

Determine the Scope of a Problem

Next, you need to find out whether anyone else is unable to FTP to Host Z. If others can FTP to Host Z (for the sake of this example, assume that they can), you can be pretty sure that the problem is specific to the user, either on their station or on the destination host. This step determines the scope of the problem and helps to differentiate between a user-specific problem and a more widely spread problem. Figure 1.5 shows that other hosts can FTP to Host Z without any problems.

Now that you have the problem narrowed down to a single user, you need to define the *boundary of dysfunctionality*. The boundary of dysfunctionality is the limit or scope of the network problem. For example, a distinction can be made between where nodes are functioning properly and where they are not. To define this boundary in our example, you need to know whether the user can successfully FTP anywhere.

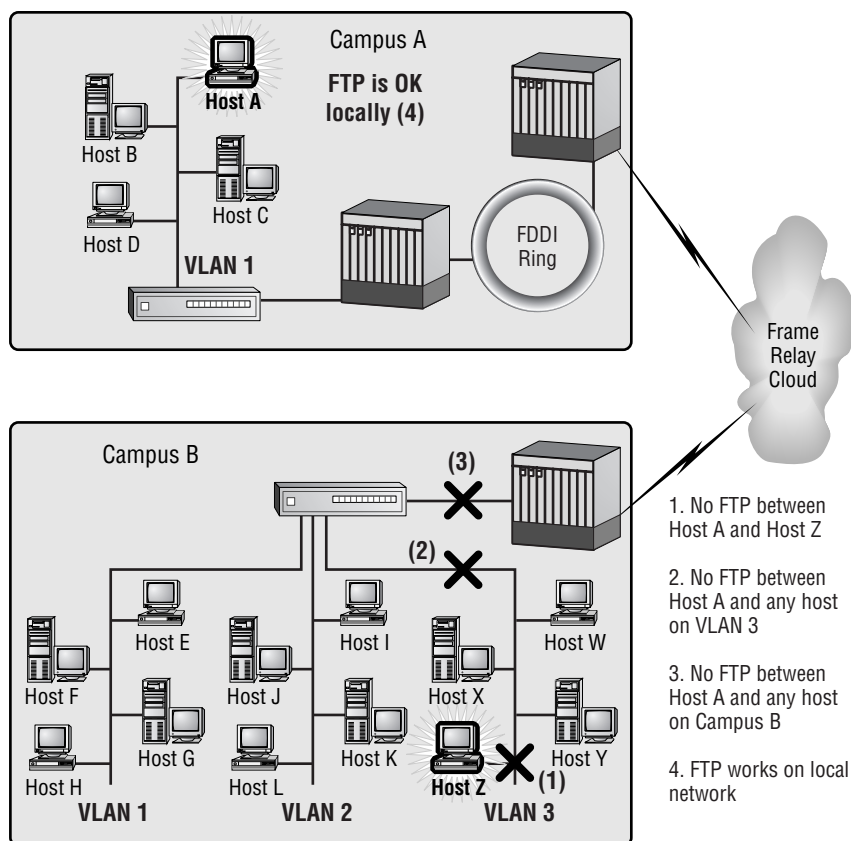**F I G U R E   1 . 5**   Other hosts can FTP to Host Z
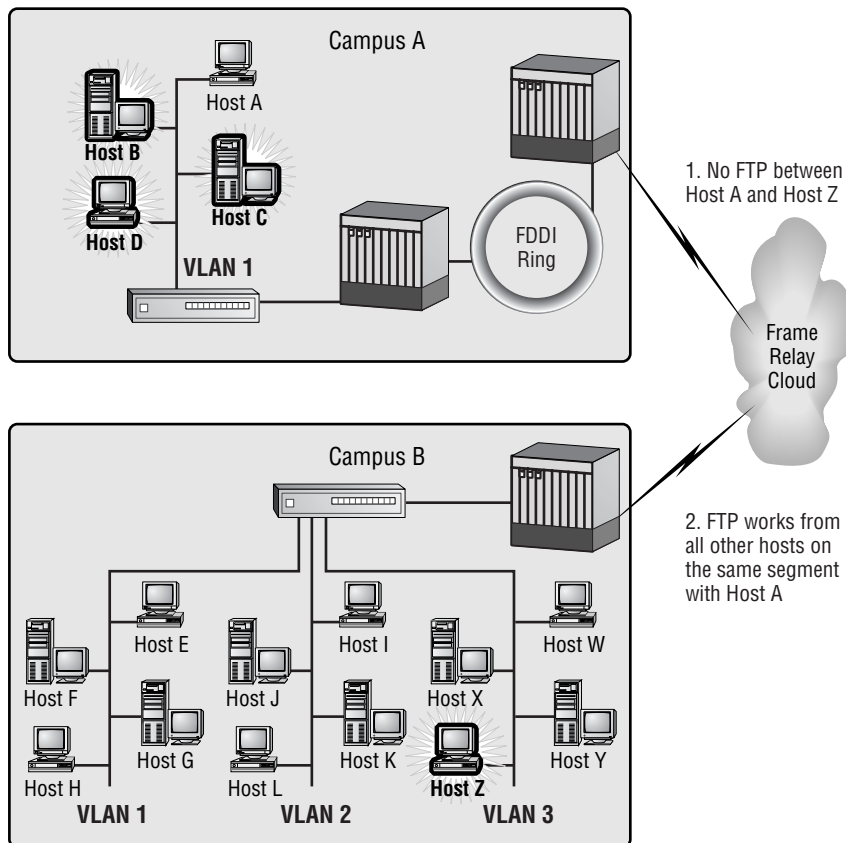
There are three methods for establishing the boundary of dysfunctionality: outside-in troubleshooting, inside-out troubleshooting, and divide-by-half troubleshooting. Each of these techniques has its own advantages and disadvantages based on the situation. The methods are explained in the following sections.

Outside-In Troubleshooting

The first method, *outside-in troubleshooting*, consists of starting the troubleshooting process at the opposite end of the connection. In this case, you would start at Campus B, VLAN 3, and work back toward the user's system (see Figure 1.6). The corresponding test would be for the user to try to FTP to another host on the same VLAN as Host Z, indicated by the X (2) on the diagram. If the result of that test is negative, then you need to come back one step. By coming back one step, you would try to FTP to a host on a different VLAN, indicated by the X (3) on the diagram. If that test failed, the only thing left to try would be to FTP to another host on the user's segment. In the example, assume that the user can FTP to other hosts that are directly connected to the same Ethernet segment. In general, outside-in troubleshooting is a good method to use when there are many hosts that cannot connect to a server or subset of servers.

FIGURE 1.6 Starting from the outside and working in

1. No FTP between Host A and Host Z

2. No FTP between Host A and any host on VLAN 3

3. No FTP between Host A and any host on Campus B

4. FTP works on local network

Inside-Out Troubleshooting

The second method of fixing the boundary of dysfuncionality is to start near the user and work your way toward the destination, Host Z in this case. This is referred to as the *inside-out troubleshooting* method. Figure 1.7 contains a diagram that describes this testing method. You see that the user can FTP to hosts within the same network, but can't FTP to any host on the Campus B network. The steps are marked by the Xs, with the step number in parentheses.

Using the second method saved you one step—three instead of four. Statistically, however, you isolate the boundary with fewer steps by using the first method. The important thing is that the boundary be established.

FIGURE 1.7   Starting from the inside and working out